

Co-regulating Internet security: the London Action Plan

Ian Brown¹
Oxford Internet Institute
University of Oxford
1 St. Giles'
Oxford OX1 3JS
United Kingdom

Christopher T. Marsden²
Department of Law
University of Essex
Wivenhoe Park
Colchester CO4 3SQ
United Kingdom

Introduction

Although the Internet with its associated information infrastructure is robust, it retains security vulnerabilities in:

- Content (software vulnerabilities, security breaches in important organisations)
- Physical structure (fibre optic infrastructures, availability of communication links and vulnerability of major elements to man-made or natural disasters).
- Distributed Denial of Service (DDoS) attacks, beginning in 2001 against Yahoo! and eBay
- Corporate responses to the increasing financial returns for attackers (for example the growth of 'phishing', malware and extortion attacks against gambling websites)

The general public, ICT specialists, industry and government perceive security threats differently. For instance, consumers' participation and behaviour on-line are distorted by concerns about identity theft, spam and denial of service. Industry has tended to focus more on the problem of sustaining infrastructure integrity in the face of increasing openness in the technical architecture and rapidly rising levels of use. Concerns belonging to (though not always embraced by) the public sector include both principled and pragmatic consequences for trust and confidence of malicious and damaging activities. The relative neglect by private parties of the consequences of e.g. privacy breaches and "phishing" can threaten 'public goods' from the rule of law to international economic competitiveness.

New approaches to this problem require public, private and civil society organisations to collaborate in new institutions of Internet governance. In addition to overlapping interests, they have complementary competences: the state has power to regulate many areas of civic and business life; business has the technical and organisational scope to change products, services and processes; and citizens can take detailed personal or community responsibility, implementing precautions that would be oppressive at national or market level and acting as trip-wires for emergent threats.

International bodies can also encourage shared approaches and solutions that markets cannot or will not provide unaided. The London Action Plan (LAP) on Spam is one such group, established in 2005 and comprising over forty government agencies (typically the consumer protection agency) from Europe, North America and Asia, and over twenty multinational companies involved in supplying security hardware,

¹ Research fellow at the Oxford Internet Institute

² Lecturer in Law and 2007-8 Co-Director, LL.M. Programme on Information Technology, Media and Entertainment Law, University of Essex. Comments welcome at: ctmarsden@yahoo.co.uk.

software and services. The LAP is a loose coordination mechanism sitting above bilateral, multilateral and standards-based initiatives, providing coordination and exchange of best practice.

In this article we have used existing literature, a large-scale electronic survey of stakeholder participants, an expert workshop and interviews with a range of LAP stakeholders to answer the following research questions:

- Where should action on Internet security sit in the continuous spectrum from self to co-regulation to ‘full’ regulation?
- How are divergent national approaches accommodated, with shifting alliances between government, industry groups and users?
- How well does the London Action Plan framework include all stakeholders, including civil society?
- What lessons can we learn from the London Action Plan for the development of other self/co-regulatory organisations?

Internet security and multi-stakeholder international governance

For government to learn how to ‘regulate reflexively’, in the expression of pioneering regulatory theorists Ayres and Braithwaite (1992), is a critical test of their competence. The test for users, governments and corporations is to arrive at acceptable joint solutions to produce innovation and dynamic freedom with greater accountability and legitimacy to society. There are excellent reasons not to regulate, because unless harm is shown, the precautionary principle is more important in Internet policy than others. It is ‘born global’, in the sense of multinational companies rather than truly global phenomena, and therefore has been adopted internationally with US technological and social norms, accompanied by US free speech philosophy and to some extent engineering to reinforce that end-to-end uncensored mode (due as much to its university origins). The Internet is increasingly relevant for students of international organizations, with the struggle over the ‘Washington consensus’ now taking place in the United Nations. This new combination of multi-stakeholder self-appointed consumer-citizen lobbies, and the challenge to US hegemony over Internet design, is used by others to press for reform of the system. Our intention is not to map such a debate – that had been done exhaustively by others – nor to broaden it to encompass the debate in the UN as an example of multi-stakeholderism – again exhaustively documented.

The US government supports bottom-up private sector-led initiatives for a useful analysis of what they see as solutions to complex problems:

“Spam: Increasingly, spam is, in large part, a security issue: spam is one way in which viruses and other security threats can be delivered to computers. Industry must play a lead role in developing technical tools to address this problem. In addition, many of these security threats often result from criminal conduct. The Convention on Cybercrime provides a comprehensive framework to address these threats. In 2003, the United States enacted an anti-spam law established a framework of civil and criminal enforcement tools to help America’s consumers, businesses, and families combat unsolicited commercial e-mail. However, the United States does not believe that the statute alone will solve spam. The United States approach to combating spam relies on a combination of legal tools for effective law enforcement, development and deployment of technology tools and

best practices by the private sector, and consumer and business education. We believe that work undertaken to combat spam should ensure that email continues to be a viable and valuable means of communication. Governments have a role to play in educating consumers and enforcing spam laws. To this end, governments should encourage spam enforcement agencies to join the London Action Plan on international spam enforcement cooperation.” (Comments 2005 at 3)

The European Union has stated:

“That stability, dependability and robustness of the Internet remain a high priority; security and spam are important issues in this field. A global common understanding of the issue of Internet security must be developed. This includes the use of security policies in general at all relevant levels.

With regard to spam there is a need to adopt common principles of action concerning cooperation in this field. Anti-spam efforts should not be based only on legislation and cross border enforcement, but also on industry self-regulation, technical solutions, partnerships between governments and the Internet Community, as well as awareness-raising.

The importance of ICTs for the competitiveness of industry and therefore encourages active involvement of the private sector in the Internet governance discussions during the second phase of WSIS.” (ITU 2005)

This suggests that most developed country governments agree the Internet regulatory model is not fundamentally inappropriate but needs adaptation. We consider this in regard to an inter-governmental multi-stakeholder network – the London Action Plan – but first explain our theoretical background in three sections: regulation, governance and the Internet; co- and self-regulation; and broadband personal Internet security.

Regulation, globalisation and the Internet

The greatest, and certainly to a Westphalian nation-state-centered universe most revolutionary (Strange 1998), challenge for regulation is the increasing co-operation between national, regional and international networks of regulators, to regulate the global information society, including the Internet (Leiner et al undated). Our interest is broader than the purely technical: it is in regulation of the global information society, which Luc Soete (1997) defined as:

... the society currently being put into place, where low-cost information and data storage and transmission technologies are in general use. This generalization of information and data use is being accompanied by organizational, commercial, social and legal innovations that will profoundly change life both in the world of work and in society generally.

Trachtman (1998: 1) explained ten years ago that:

Because the technology is so exhilarating, there is a tendency to claim that the changes we do observe in sovereignty, the state, jurisdiction and law all are caused by cyberspace... it is not the state which has died, but the long-moribund theory of absolute territorial sovereignty...the correct allocation of authority is dynamic, complex and contingent ... the group of powers society decides to assign to the state at any given moment and in any given circumstance. Social institutions for allocation of jurisdiction have not changed to reflect the technological changes brought by the rise of cyberspace.

Therefore:

one may view the rise of cyberspace as a phenomenon that accentuates the old problems to a point where it is worthwhile to devise a more substantial institutional solution.

Novel experimentation has been taking place over the roles of companies, governments and consumers/citizens in debates around responsibility and the Internet (Lessig 1998). The concept of 'governance', an amorphous phrase to describe power relations differentiated from the 'hard' rules of government, became a popular catchphrase around the mid-1990s (Kooiman 2003, Kleinwachter 2004; Mueller et al 2004). Hoffman (2005, p.2) explains that Internet governance "can be understood as an open-ended, collective process of searching which aims to fill a global 'regulatory void' both conceptually and institutionally in a legitimate way. This void arose because the principle of sovereignty, which was an essential component in international regulation of the telephone network, has not been carried over to the Internet." MacLean states: "a complex and confusing array of local activities take place without any overall coherence or top-down coordination of the kind formerly provided by the United Nations" (2004, p.99).

The United Nations Secretary-General in 2004 established a Working Group on Internet Governance (WGIG) to provide some clarification of the term and the public policy issues that are relevant in this context. It reported at the second World Summit on the Information Society (United Nations 2005). Its concerns are largely technical in character, yet its central concern is absolutely clear and non-technical: Internet governance is neither an inter-governmental nor a technical nor a market-led phenomenon. It is all of these but also and critically involves the Internet user, as demonstrated in the composition of the WGIG itself (Kummer 2004). It has been extended in the work of the Internet Governance Forum which first met in Athens in 2006, meets in Rio in 2007, and then India in 2008 (See <http://www.intgovforum.org/>). Such co- and self-regulation experiments have been extended in for instance the United Nations context through CONGO (the Conference of Non-Governmental Organisations), through the Domain Name System and ICANN (the Internet Corporation for Assigning Names and Numbers: Mueller 2002), and locally through the UK regulator Ofcom, which is conducting a long-term study of such arrangements in 2007.

Regulation has many definitions, and we do not intend to draw on a particular definition to the exclusion of others. However, we do want to explain that our interest does encompass explicitly 'multistakeholderisation' (Baird 2002), though the case study is more concerned with the political economy of nation-states and globalising economic actors, the multinational corporations. The need for a fresh approach considering economic and social issues as part of technology deployment has been emphasised by the National Science Foundation in the US, with emphasis on Quality of Service and security (Marcus 2004), the approach we also adopt (Clark 2005). That clearly affects our view of regulation. Ayres and Braithwaite (1992: 3) state:

Practical people who are concerned with outcomes seek to understand the intricacies of interplays between state regulation and private orderings...If we accept that sound policy analysis is about understanding private regulation...then interesting possibilities open up to steer the mix of private and public regulation.

This paper – and previous work – attempts to interpret the interplay of neo-classical economic and normative values in the regulation of cyberspace (Kahin and Keller 1997; Kahin and Neeson 1997, Marsden 2000). In her final unfinished article, Strange (1998: 2.8) explains that, despite the static nature of much realist international relations and legal theory:

This sharp distinction between international law and domestic law, and correspondingly between international politics ... and domestic politics is being widely questioned. The evidence of overlap and of reciprocal influence is abundant.

We concur fully. If this paper has any message, it is that regulation (and hence perhaps ‘governance’) is multi-layered, in actors, methods and geographical reaches.

The idea that roles and responsibilities in a global and highly dynamic environment such as the Internet can be allocated on a temporary and contingent basis according to such inclusive and non-hierarchical relationships is not of course new. The allocation of roles has often historically been shifted between government, corporations and civil society (consider the Red Cross or the British East India Company’s histories) but it appears that the United Nations is providing a more durable multi-stakeholder relationship in regard to Internet governance, in addition to the existing ‘spaghetti soup’ of existing intergovernmental and regional fora (e.g. OECD, OSCE, Council of Europe, WTO). Its call for informal multi-stakeholder arrangements beyond the traditions of the ECOSOC (economic and social committee) arrangements that dominate post-1945 institutions such as the European Union and United Nations, is a novel and fascinating attempt to achieve real global dialogue around responsibilities in the global information society, and may be a significant new governance paradigm in the coming years.

Co- and self-regulation

In the field of Internet content regulation, there is a much more relevant and broad field of non-binding declarations and recommendations than useful statute and case law. The uses of ‘soft law’, ‘soft power’ and non-legal solutions, e.g. standards (Schmidt and Werle 1998, Reidenberg 1998), are well-known in the context of Internet development. Such ‘soft solutions’ also feature large in the European and US ‘better regulation’ agenda, and the 2001 European White Paper on Governance. The non-binding policy instrument is a staple of self-regulation backed by the threat – but not implementation – of specific legal authority to impose direct state regulation (Scheuer 2006). The pitfalls as well as advantages of self-regulation are highlighted by Pitofsky (1998):

“From a public policy perspective, self-regulation can offer several advantages over government regulation or legislation. It often is more prompt, flexible, and effective than government regulation. Self-regulation can bring the accumulated judgment and experience of an industry to bear on issues that are sometimes difficult for the government to define with bright line rules. Finally, government resources are limited and unlikely to grow in the future. Thus, many government agencies, like the FTC, have sought to leverage their limited resources by promoting and encouraging self-regulation.”

Improving regulation was the specific concern of the Mandelkern (2001) Group on Better Regulation, a panel of consultants appointed to review implementation of the conclusions of the European Council Lisbon summit in 2000. In considering “co-

regulation” as an alternative regulatory format, this report highlights the responsibilities undertaken by private actors, whose role can both be “top down” as original rule-makers, or “bottom up”, implementing state rules in what Mandelkern called the “cooperative approach”. The European Commission (2001) Governance White Paper explained: “the quality, relevance and effectiveness of EU policies depend on ensuring wide participation throughout the policy chain – from conception to implementation. Improved participation is likely creating more confidence in the end result and in Institutions which deliver policies.” The White Paper does suggest a “more effective and transparent consultation at the heart of E.U. policy-shaping” through what we might now term ‘multi-stakeholder governance’: advisory committees, hearings, on-line consultations. This led to the European Commission (2003a) Inter-institutional Agreement on Better Law-making. The Agreement imposes certain limits to these alternative modes of regulation: the use of co-regulation or self-regulation must: always be consistent with Community law, meet the criteria of transparency (in particular the publicizing of agreements) and representativeness of the parties involved, representing added value for the general interest. The text requires stakeholder representation and the transparency of the procedures followed within the self- or co-regulatory process. The mechanisms may be used on the basis of criteria defined in the enabling legislation. Finally, the added value of alternative regulation mechanisms relies on flexible and efficient enforcement mechanisms, including labelling, standardisation or Alternative Dispute Resolution (ADR).

Millwood-Hargrave (2007) graphically represents the spectrum from state regulation to self-regulation (as shown in Figure 1) referring to co-regulatory institutions, industry-wide self-regulation and individual service provider schemes.

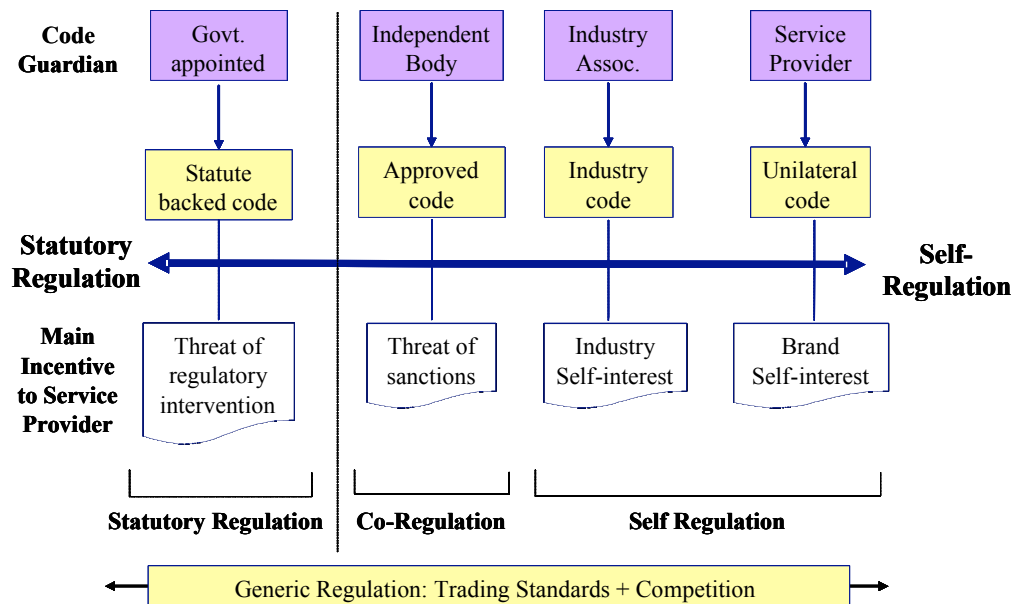


Figure 1: Millwood-Hargrave Diagram of regulatory type and incentive structure

Consider a continuum from state regulation to co-regulation and ‘regulated self-regulation’ to self-regulation, and on to standard setting and regulation by individual communities and by norm setting (Posner 1984, Ogus 1994, Baldwin et al 1998, Gaines and Kimber 2001). We can identify self-regulatory arrangements whose modus operandi consist of non-binding norms of action, process and behaviour, for

whom sanctions of the formal regulatory type play no part. Self- and co-regulation features include:

- Locational diversity: regional, global, national schemes play interdependent roles (Thierer 2004, Zittrain 2003);
- Different regulatory systems between co- and self-regulation with terminological confusion between schemes by sector and country (Schulz and Held 2001);
- ‘Multi-stakeholderism’: Institutions encompassing public and private sector actors, and civil society stakeholders.

Self-regulatory institutions by rule or the formation of norms exercise a function that shapes or controls the behaviour of actors in that environment. Kleist and Palzer (2007) explain that path dependence is key to understanding the perception of national and sectoral co-regulatory schemes:

“Where prior to considering co-regulation there had been a strict command-and-control regulation, co-regulation comes as a form of liberalisation and, as a rule, will be applauded by the industry. In contrast, where voluntary self-regulation had been paramount, any debates on co-regulation might be seen as the state “capturing” the respective self-regulator.”

In this article, our interest is in the degree to which consumers are formally recognised in such schemes, with particular reference to the Internet security theme. A common understanding of the concept of co-regulation, its importance for regulators, and the perspective with which to assess its impact are among the most important threshold issues to address, before it is possible to consider specific regulatory responses (Goldberg, Prosser and Verhulst 1998). Currently, however, as has been noted (Senden 2005) there is some uncertainty as to the precise scope of the terms self-regulation and co-regulation.

Broadband personal Internet security

The security threats from spam, viruses and Denial of Service (DoS) attacks mean the public Internet is fragmenting fast, with firewalls driving a segmentation of the public Internet (Crowcroft and Philips 2001; Eltzroth 1999). The techno-economic arguments for faster progress in Internet development relies on development of the logical layer – the Internet protocols. The need for a halt to the levels of viruses, Trojans and particularly hijacked networks of Personal Computers (PCs) is immediately apparent (Edwards 2006). The size of “botnets” of compromised machines has reached the millions, in the case of a 2005 Netherlands-based hacker. The estimates for the percentage of email that is spam are in the 55-75% range. However, this is generally pre-filtered by Internet Service Providers (ISPs), with 80% of all email sent to AOL members removed as spam in 2005. In Anglo-Saxon countries, with highly efficient spam filtering systems in place, spam concerns peaked in late 2003 and have since subsided (AOL Time Warner 2005). Of continued and rising concern are the more sophisticated types of Internet crime, especially those involving distributed attacks using ‘hijacked’ PCs.

Most sectors of the information infrastructure are privately owned and cannot be controlled by governments deciding what levels of connectivity or security should be available. Companies and individuals ultimately decide what levels of broadband speed they want, and the risk they will tolerate, and thus what level of security

“interference” they are prepared to accept, as well as broadband speed for which they will pay.

International bodies such as the International Chamber of Commerce, Organisation for Economic Co-operation and Development, European Union, Council of Europe and G8 can also encourage shared approaches and solutions where markets cannot provide on their own. The WSIS, as well as its forerunner the Digital Opportunities Taskforce, and the Global Alliance for ICT and Development are also engaged in ensuring that multi-stakeholder discussions take place around these vital issues. As broadband networks and their security form the basis for the networked ICT applications that drive the Information Society, it is unsurprising that the governance of these networks is increasingly a subject for a broader public policy debate.

The developed world’s increased dependency on ICT and the high degree of integration in all aspects of our lives – economic, social, administrative, and so on – throw into acute relief the importance of providing for security. Even as organisations and consumers are getting used to the most recent technological development and devising ways to meeting the challenges presented, criminals stay one step ahead of the game: P2P networks are ideal for hiding illegal content, “phishing” takes advantage of our trust in electronic communications and mobile phones have become attractive targets for street robbery (phishing involves sending apparently legitimate e-mails which deceive victims into submitting sensitive personal or financial data to a website which appears to be legitimate but is, in fact fake). The general public perceives security threats differently to specialists in the ICT industry or the government. To business, sustaining the integrity of the infrastructure and coping with rapidly rising usage are major concerns. The Internet was designed to automatically divert around problems or outages, giving the network a unique property of resiliency, and an ability to withstand random attacks or disruption. Although the Internet and its associated information infrastructure is clearly a global phenomenon, it is uniquely vulnerable in local ways, for instance because it is end-to-end and anonymous – a virus attack uses the same powerful properties of the Internet that make its other uses so compellingly beneficial.

Network security requirements at European level must be implemented in national law. They impose costs on the network in addition to existing costs for spam filtering and protection against Distributed Denial of Service (DDoS) attacks, phishing and other crimes that Internet Service Providers typically incur in order to protect their subscribers from the worst excesses of Internet abuse. Businesses also have an internal responsibility to keep data they use, in whatever form, safe and secure. If not managed properly, the risks stemming from poor data security practices and global vulnerabilities as described above serve to undermine trust and confidence in the Internet. This is a growing problem as dependence on broadband (as a key element of the critical information infrastructure) grows and as ICT moves towards pervasive computing, and the ‘Network of Things’ (ITU 2005a). There is an escalating ‘arms race’ as attack and opportunistic behaviour become more sophisticated (Brown, Edwards and Marsden 2006).

The responses are a mix of technological and ‘soft’ strategies, developed and deployed at both individual enterprise and wider levels. These include protected ‘walled garden’ environments with users kept behind their ISP’s ‘firewall’ or even the national ‘Great Firewall of China’, and the security of corporate Virtual Private Networks. A potential loss of Internet openness and end-to-end connectivity is one

potential casualty of security concerns. Another is privacy, which in some ways is the mirror of security. There are differences between the developed and developing world, which are significant both in terms of the coherence and pace of technological development and because these worlds interact strongly (with hackers residing in Ukraine or North Korea, for example, while spammers use the hijacked computers to send spam from Florida).

Addressing this problem is not within the powers of any one sector or organisation. Solutions require public and private organisations to collaborate with each other and with citizens. Industries and businesses have the technical and organisational scope to change products, services and processes. The state has the power to regulate areas of life and business. The citizen, too, can take some responsibility. For instance, the main source of vulnerability to DDoS attacks is unprotected home computers connected to high speed, always on broadband links. Resolving this requires a mix of consumer responsibility (keeping computers protected and up to date), industry action (for example, Internet Service Providers using methods to mitigate the effects of such attacks), and government action (adjusting criminal law to make such activities punishable, and trying to ensure robust enforcement).

Related Initiatives

Initiatives to tackle spam and related security issues run the full span of the regulatory spectrum, from government-led action, through co-regulatory institutions such as the London Action Plan, to self-regulatory industry groups.

During 2007 the Organisation for Economic Cooperation and Development and APEC are researching an Analytical Report on Malicious Software that will inform the OECD ministerial meeting on the Future of the Internet Economy in Seoul next year. This builds upon OECD-APEC workshops in 2006 and 2007 on the problem. The report will provide information on malware, the malware economy and possible incentives and disincentives in these markets (Carblanc 2007).

The International Telecommunications Union Development sector is carrying out a work program between 2007—2009 to assist developing countries with cybersecurity. As well as specific anti-spam measures this will include more general capacity-building and monitoring initiatives and foster regional cybersecurity cooperation (ITU-D 2007).

European data protection authorities meet regularly in the Article 29 Working Party set up by the EU Data Protection Directive, and have collectively developed opinions and recommendations on spam-related subjects, most recently on the adequacy of their enforcement powers within the European legal framework (Art. 29 WP 2006). Many of these authorities are also members of the European Contact Network on Spam Enforcement, set up by the European Commission (EC 2004), which has further agreed to share information and pursue complaints across member-state borders. The European Network and Information Security Agency (ENISA) has also undertaken a survey of ISPs and regulators on the measures they have taken under the European telecommunications privacy framework (ENISA 2006), which is being repeated during 2007.

The e-crime dimension of the EC is controversial, given acknowledged flaws in the EUROPOL system and the role of the Council of Europe Convention on Cybercrime. Member States including the Slovak Republic have previously criticised the First Pillar approach (which allows decisions short of consensus, unlike the Third Pillar

which arguably was more intended to serve as the instrument for pan-EU criminal enforcement) to the Data Protection Directive, and it can be anticipated that more resistance will be offered to the idea of any new cybercrime legislation.

One of the other significant activities at the European level is the Task Force Computer Security Incident Response Team (TF-CSIRT), a Task Force of the Trans European Research and Education Networking Association (TERENA). TF-CSIRT supports the co-ordination of CSIRTs from both private and public organisations across Europe and also runs a number of relevant activities, including the Trusted Introducer program (where existing members of TF-CSIRT can ‘nominate’ other teams that are not yet members) and the TRANSITS (Training Course for Incident Response Teams). The global FIRST (Forum of Incident Response Teams) has recently signed a Memorandum of Understanding with the TRANSITS programme, to jointly develop the syllabus for CSIRTs and CERTs (TERENA 2006).

More direct regulatory action is being undertaken by government agencies such as the Australian Communications and Media Authority, who recently prosecuted a major spammer that was subsequently fined AUS\$4.5m. ACMA’s SpamMATTERS reporting facility, which allows members of the public to report spam messages using software plugins for mail software such as Microsoft’s Outlook, was used by 207,000 people to report 25m messages in its first year. ACMA have also funded a four-year initiative to report compromised machines to 25 Internet Service Providers (Duffy 2007b).

The London Action Plan has influenced and been influenced by the design of co-regulatory regional anti-spam initiatives. In 2005 regulators from nine Asia-Pacific countries along with three industry associations signed the Seoul–Melbourne Anti Spam Memorandum Of Understanding. This set up a structure with very similar aims and procedures as the LAP, including information sharing, points of contact and regular online and physical meetings (Duffy 2007c).

At the self-regulatory end of the spectrum, the most significant global industry anti-spam and security initiative is the Messaging Anti-Abuse Working Group. MAAWG has over 100 members including ISPs responsible for operating over 750 million mailboxes. The group has developed a number of technical recommendations for its operators such as a code of conduct for message system operators and sender best communication practices (Jones 2007). MAAWG is mirrored by national industry associations such as the Japan Email Anti-Abuse Group, which has 30 company members and 2 government observers and undertakes similar activities to MAAWG at the national level (Sakuraba 2007).

London Action Plan: Legal Context, Activities and Achievements

The London Action Plan (LAP) on International Spam Enforcement Cooperation is an agreement between public agencies from 27 countries concerned with reducing unsolicited commercial e-mail messages. It includes data protection authorities, telecommunications regulators and consumer protection bodies. Companies such as Telefonica, Microsoft and the London Internet Exchange also participate.³ The Plan’s aim is “to promote international spam enforcement cooperation and address spam-related problems, such as online fraud and deception, phishing, and dissemination of viruses.” (FTC 2004).

³ A full list of participants is at <http://londonactionplan.org/?q=node/5>

Duffy (2007a) summarised the problems that led to the formation of the Plan as follows:

- Governments are faced by a fast-changing, global Internet that in turn is speeding up the process of globalisation.
- The Internet has no borders, border patrols or single laws.
- Spam and related problems have demonstrated the limits of national law and law enforcement.

Each participating government agency agrees to nominate a point of contact for enforcement communication, and to encourage communication across national government on this issue; to take part in quarterly conference calls; and to support the involvement of less developed countries. Private sector representatives similarly agree to nominate a point of contact; encourage cross-industry communication; report into select conference calls; and assist in training. Companies invited to participate include “financial institutions, Internet service providers, telecommunications companies, information security software providers, mobile operators, courier services, commercial mail receiving agencies, industry membership organizations, consumer organizations, payment system providers, credit reporting agencies, domain name registrars and registries, and providers of alternative dispute resolution services.” A new company participant may be vetoed by a member agency (FTC 2004).

Members of the Plan have recently held teleconferences every two months, and met for the fourth time in Washington DC in October 2007 (de Natris 2007). Current agency participants are from Australia, Belgium, Canada, Chile, China, Denmark, Finland, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, the Netherlands, Nigeria, Norway, South Korea, Spain, Sweden, Switzerland, Taiwan, the United Kingdom and the United States. Private sector participants are from Australia, Belgium, Canada, Chile, China, France, Germany, Hong Kong, Malaysia, Spain, the United Kingdom and the United States. There are observers from Belgium, France, Russia and the United Kingdom.

The Plan builds on anti-spam work by the OECD Spam Task Force, the International Telecommunications Union (ITU), the European Union (EU), the International Consumer Protection Enforcement Network (ICPEN), and the Asia-Pacific Economic Cooperation (APEC). Participants met in London on 11 October 2004 to discuss international collaboration, publishing an initial agreement (FTC 2004) and opening it for signature by other anti-spam entities. Plan members are keen to maintain the flexible nature of their cooperation, rather than developing a more political treaty-based approach.

Plan members are keen to involve other government agencies, Internet Service Providers and relevant parties from around the world in their work. While most governments maintain or sponsor Computer Emergency Response Teams, these do not tend to include policymakers, and hence are not on their own broad enough to cover the work of the LAP in each nation (Sahel 2007). Further resources would allow the engagement of consultants to undertake work such as surveys of members. Such resources would be more likely to come from private sector participants than government agency members.

Design and organisation of the institution

The London Action Plan secretariat is hosted by the UK Office of Fair Trading and the US Federal Trade Commission, and is contactable by e-mail. The Plan has no formal budget. Participating organisations' staff undertake activities on a best-efforts basis. As an example, there are between 10—15 people across the UK government with some involvement in the Plan (Sahel 2007). In general each participating agency has two members of staff involved. They also provide resources to host meetings and conferences.

In some senses, the LAP acts as an informal mutual legal assistance mechanism. It builds trust between participants as they exchange information, helping government agencies to shut down foreign sources of spam (Sahel 2007). Governments receive information on the effects of legislation, new threats and the results of their efforts. Businesses share data and experience (de Natris 2007).

The London Action Plan has been successful in building cooperation across its participant nations and shutting down significant spam sources; but its members do not keep detailed statistics. Developing trust across governments and the private sector is a key goal. Duffy (2007a) summarised the main benefits of the Plan so far as follows:

- Enforcement personnel are put into direct contact with each other.
- Government participants gain valuable information on the effects of law, needs of enforcement agencies, statistics on problems, new threats and the results of enforcement activity.
- Private business shares data and experience on the problem and responses.

Members have also cooperated with the OECD on a survey of malicious software and the value chain behind organised crime involvement in online scams. This included pinpointing the actors involved and how they communicate, giving some options by which law enforcement agencies can disrupt these activities (Sahel 2007).

Conclusion

We return to first principles: what is wrong with Internet security and what is being done about it by governments? What regulatory structures can perform more efficiently and accountably than the devolved heterarchical self-regulatory structures that currently exist? Unless we can find a cure better than the disease, change is neither inevitable nor beneficial.

An unstoppable force is colliding head-on with an immovable obstacle. Legitimate, accountable bureaucratic governments are standing in the way of the dynamic, innovative, laissez-faire Internet 'netizens'. After a laissez-faire period in which government acted as enabler of Internet development across boundaries and encouraged its increased use, security and competitive provision, the new world order post-9/11 has resulted in a renewed attempt by governments to impose control on the newly pervasive Internet. With a billion citizens online, and over a billion soon to join via mobile telephones, both developed and developing countries are asserting national sovereignty over Internet content, allocation of Domain Names, and design. From Australian and French government intervention to prevent hate speech and pornography online, to the 'Great Firewall' of China designed to stop the global Internet contaminating the one-party dictatorship in the world's most populous nation, to United States anti-infringement rules that criminalise children and innovators, to

attempts to preserve local cultures in the face of the global onslaught of the “Californication” of values, the regulation of the Internet has continued.

As the immovable object determines its strategy towards the Internet, we can pose a series of governance questions. Governments intend to regulate the fastest growing and most powerful information resource in the history of the world, a seamless end-to-end web of computers, data and people. Will they find a new flexibility in their bureaucracies to cope with the evolution of this extraordinary organism?

1. Can the governance response be dynamically legitimate and can the Internet be permitted to continue its legitimate dynamism?

Problem: governance by legislation and international treaty involves a six-year policy cycle, and six years prior to WSIS, in 1997, broadband was still a laboratory experiment. Embracing the speed of Internet development is a major problem for largely static government bureaucracies.

2. Can the governance response be innovatively accountable, and will the Internet pioneers be accountably innovative?

Problem: governments derive their legitimacy from periodic general elections, approximately every four years, from which they build coalitions of interests at national and international level to regulate in the interests of the majority. Four years prior to WSIS, in 1999, the global Internet population was only 100million, mainly in North America. Now, in 2007, it is over a billion, with the largest constituency in Asia. Representation in governance is therefore an enormously challenging task. On the other hand, the builders of the Internet were a group of middle-class white males from Anglo-Saxon cultures with a clearly libertarian political ethos, and they continue to govern the architecture of the Internet, no matter how ethnically, sexually and age-diverse its growing population has become.

3. Can the governance response be a benevolent control, and can Internet users be responsibly free?

Problem: government is rules-based, and the bureaucratic method is to systematize the object to be controlled within bureaucratic definitions: what systems theory after Niklas Luhman describes as an autopoietic self-referential system. In brief, government is a hammer, and to a hammer everything else looks like a nail.

As for a specific solution to security concerns, we can identify short-term solutions such as CERTs and ISP activities, medium-term solutions such as upgraded vendor solutions and law enforcement including the LAP, and longer-term goals based on new standards and protocols. The short- and medium-term solutions are already taking place in broadband ISPs, with ‘packet sniffing’ via dedicated high-speed appliances. Messaging providers commonly set filtering rules for executable program attachments and other potentially dangerous e-mail content, though as with all forms of filtering or censoring, the technology and design will enable only as much accuracy as the prior rules.

Longer-term, Clark (2005) describes a four-stage development required:

1. “Give the medium a basic security architecture -- the ability to authenticate whom you are communicating with and prevent things like spam and viruses from ever reaching your PC.

2. “Make the new architecture practical by devising protocols that allow ISPs to better route traffic and collaborate to offer advanced services without compromising their businesses.
3. Allow future computing devices of any size to connect to the Internet -- not just PCs but sensors and embedded processors.
4. Add technology that makes the network easier to manage and more resilient. For example, a new design should allow all pieces of the network to detect and report emerging problems – whether technical breakdowns, traffic jams, or replicating worms – to network administrators.”

Clark is proposing the introduction design principles for a more filtered Internet, with the potential for a change from a ‘best effort’ end-to-end design that has no quality of service and total anonymity, to a more graduated design with authentication. This profoundly alters the nature of the network, and creates the probability of widespread packet discrimination based on security, speed, cost and other considerations.

Self and co-regulatory systems do not operate in a vacuum. There needs to be a synergy between regulatory frameworks and self-regulatory systems, because of the complexity of pathologies and complexity of the heavily distributed organizational structure of Internet. Personal internet security is a complex area and very often there is no understanding of the implication of the fact that organizations responsible for it are very often not the same ones which suffer the consequences. Although self-regulatory systems are in a sense industry-driven, they can be helped by the existence of a legal framework – even though they can still exist in the absence of such a framework. The force of the law is of variable benefit to new regulatory systems, in particular those which address new problem areas.

Acknowledgements

The authors are grateful for advice from Jeanette Hoffman, Adam Peake, Lilian Edwards, Richard Clayton, Bernard Benhamou, Tim Kelly, and participants at the European Consortium of Political Research annual conference, Budapest, Hungary, September 2005. Marsden also wishes to thank former colleagues at RAND Europe: Maarten Botterman, Jonathan Cave, Constantijn Van Oranje-Nassau, Neil Robinson, Lorenzo Valeri, UK government officials Martin Boyle and Jean-Jacques Sahel.

References

AOL Time Warner (2005) Press Release
http://media.timewarner.com/media/newmedia/cb_press_view.cfm?release_num=55254499, 28 December 2005.

Article 29 Working Party (2006) Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, adopted 26 September 2006. Available from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

Ayres, Ian and John Braithwaite (1992) Responsive Regulation: Transcending the Deregulation Debate O.U.P.at 3.

Baird Zoe (2002) Governing the Internet: Engaging Government, Business, and Nonprofits, Foreign Affairs, November/December 2002

Baldwin, R., C. Hood and C. Scott (1998) Socio-Legal Reader on Regulation, Oxford: Oxford University Press

Brown, I., Edwards L. and Marsden, C. (2006). *Legal and institutional responses to Denial of Service Attacks*. Communications Research Network/Department for Trade and Industry joint seminar on Spam/DDoS, 13 November, at <http://www.communicationsresearch.net/events/article/default.aspx?objid=1464>

Carblanc, Ann (2007) OECD – APEC Work on Malicious Software, Presentation to Asia Pacific Coalition Against Unsolicited Commercial Email, New Delhi, 1 September 2007. Available from <http://wiki.apcauce.org/rup2007/AC-Delhi-OECD%20presentation%20on%20Malware.pdf>

Clarke, D. (2005) FIND and Architecture: A new NSF initiative, at http://find.isi.edu/presentation_files/Clark_Arch_Security.pdf

Clayton, Richard (Cambridge University Computer Laboratory) (2007) Face-to-face interview, 21 September 2007. Interviewer: Ian Brown

Comments of the United States of America on Internet Governance, 15 August 2005, at www.state.gov

Crowcroft, J. and Philips I. (2001) *TCP/IP & Linux Protocol Implementation: Systems Code for the Linux Internet*, Wiley & Co.

de Natris, Wout (2007) Presentation to the Council of Europe, 12 June 2007. Available from http://www.londonactionplan.org/files/LAP_june2007.ppt

Duffy, Chris (2007a) The London Action Plan, Presentation to Asia Pacific Coalition Against Unsolicited Commercial Email, New Delhi, 2 September 2007. Available from http://wiki.apcauce.org/rup2007/LAP_presentation%20India%202007%20-%20revised%20Australia.pdf

Duffy, Chris (2007b) Australian Communications and Media Authority – Regional update, Presentation to Asia Pacific Coalition Against Unsolicited Commercial Email, New Delhi, 2 September 2007. Available from <http://www.apcauce.org/wiki/rup2007/ACMA%20regional%20update%20August%202007.pdf>

Duffy, Chris (2007c) Seoul–Melbourne Anti Spam MOU, Presentation to Asia Pacific Coalition Against Unsolicited Commercial Email, New Delhi, 2 September 2007. Available from <http://wiki.apcauce.org/rup2007/Seoul%20-%20Mel%20MOU%20presentation%20India%202007.pdf>

EC (2004) Communication COM(2004) 28 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or ‘spam’, adopted 22 January 2004.

Edwards, Lilian (2006) Chapter 2 in Edwards, L. (ed) (2006) *The new Legal Framework for E-Commerce in Europe*, Hart Publishing, Oxford, at <http://www.hart.oxi.net/pdf/1841134511.pdf>

Eltzroth, Carter (1999) *E-Commerce: Open for Business*, Study on the Classification of Standardisation Requirements in Electronic Commerce for World Bank and the European Commission DG MARKT

ENISA (2006) *Security and Anti-Spam Measures of Electronic Communication Service Providers – Survey*, ENISA/TD/SP/06/55, February 2006. Available from http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf

- European Commission (2001) *Governance White Paper* COM (2001)428 final
- European Commission (2003a) *Inter-institutional Agreement on Better Law-making* of 16 December 2003, OJ 31.12.2003, 2003/C 321/01
- Federal Trade Commission (2004) *The London Action Plan On International Spam Enforcement Cooperation*, 11 October 2004. Available from <http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf>
- Gaines, Sanford E. and Cliona Kimber (2001) *Redirecting Self-Regulation*, *Env. Law* 13(157) 267-275
- Goldberg D., Prosser T. and Verhulst S. (1998) *Regulating the Changing Media: A Comparative Study*, Oxford: Oxford University Press.
- Hoffman, J. (2005). *Internet Governance: A Regulative Idea in Flux*. Paper presented to European Consortium of Political Research, Budapest, September 2005.
- ITU (2005) 1 August, WSIS-II/PC-3/CONTR/19-E, Initial comments by the European Union and the acceding countries Romania and Bulgaria, on the report of the Working Group on Internet Governance.
- ITU (2005a) *Internet Reports: The Internet of Things*. At <http://www.itu.int/osg/spu/publications/internetofthings/>
- ITU-D (2007) *ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009*, 11 July 2007 draft. Available from <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf>
- Jones, Mike (2007) *MAAWG Update to APCAUCE*, Presentation to Asia Pacific Coalition Against Unsolicited Commercial Email, New Delhi, 2 September 2007. Available from <http://www.apcauce.org/wiki/rup2007/MAAWG%20-%20APCAUCE%20preso.pdf>
- Kahin, B. and Nesson C. eds.(1997) *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, Cambridge MA: MIT Press
- Kahin, Brian and Abbate, Janet eds. (1995) *Standards Policy for Information Infrastructure*, Cambridge MA: MIT Press.
- Kahin, Brian and Keller, James H. (eds)(1997) *Coordinating the Internet*, Cambridge MA: MIT Press
- Kleinwächter, Wolfgang (2004). *Internet Co-Governance – Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation*. Paper presented at the Informal Consultation of the Working Group on Internet Governance (WGIG), Geneva, September 20–21, 2004 at <http://www.itu.int/wsis/preparatory2/wgig/kleinwachter.doc>
- Kleist, T. and Palzer, C. (2007). *Co-Regulation as an instrument of modern regulation*. Working Paper in preparation of the expert seminar under the German EU presidency “More trust in contents – The potential of co- and self-regulation in digital media” Leipzig, 9-11 May 2007
- Kooiman, Jan (2003). *Governing as Governance*. London: Sage.
- Kummer, Markus (2004). *The Results of the WSIS Negotiations on Internet Governance*. In D. MacLean (Ed.), *Internet Governance: A Grand Collaboration* (pp. 53-57). New York: United Nations ICT Task Force Series 5

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet," www.isoc.org/internet/history/brief.html

Lessig, L. (1998). Governance. Keynote speech at CPSR Conference on Internet Governance, October 10, 1998, at <http://www.lessig.org/content/articles/works/cpsr.pdf>

MacLean, D. (2004). Herding Schrödinger's Cats: Some Conceptual Tools for Thinking about Internet Governance. In D. MacLean (Ed.), *Internet Governance: A Grand Collaboration* (pp. 73-99). New York: United Nations ICT Task Force Series 5. Also at <http://www.unicttaskforce.org/perl/documents.pl?do=download;id=778>

Mandelkern (2001). Group on Better Regulation. Final Report, 13 November 2001, available from <http://www.cabinetoffice.gov.uk/regulation/documents/europe/pdf/mandfinrep.pdf>

Marcus, J. Scott (2004) Evolving Core Capabilities Of The Internet, 3 J. On Telecomm. & High Tech. L. at 123-163.

Marsden, C. (ed 2000) *Regulating the Global Information Society*, Routledge, New York,.

Millwood-Hargrave, A. (2007). Presentation to the expert seminar under the German EU presidency "More trust in contents – The potential of co- and self-regulation in digital media" Leipzig, 9-11 May 2007

Mueller, M. & McKnight L. (2004). Making Sense of 'Internet Governance': Defining Principles and Norms in a Policy Context. Section 3 (pp.100-121) In D. MacLean (Ed.) ,*Internet Governance: A Grand Collaboration*. New York: ICT Task Force Series 5.

Ogus, A. I. (1994) *Regulation: Legal Form and Economic Theory*, Oxford: Clarendon Press

Pitofsky, R. (1998) Self Regulation And Antitrust, Prepared Remarks of Chairman, Federal Trade Commission, D. C. Bar Association Symposium, February 18, 1998, Washington, D.C. at http://www.ftc.gov/speeches/pitofsky/N_2_#N_2_

Posner, R. A. (1984) Theories of Economic Regulation 5 *Bell Journal of Economics and Management Science* 335

Reidenberg, J. R. (1998). *Lex Informatica: The Formulation of Information Policy Rules Through Technology*. *Texas Law Review*, 76, 3, 553–584

Sahel, Jean-Jacques (Department for Business Enterprise and Regulatory Reform, UK) (2007) Face-to-face interview, 24 August 2007. Interviewers: Ian Brown and Chris Marsden.

Sakuraba, Shuji (2007) Japan Email Anti-Abuse Group, Presentation to Asia Pacific Coalition Against Unsolicited Commercial Email, New Delhi, 2 September 2007. Available from http://wiki.apcauce.org/rup2007/JEAG_apcauce2007.pdf

Scheuer, A. (2006). Sections 5-6 in Held and Scheuer (2006) Report: Study on Co-Regulation Measures in the Media Sector; Study for the European Commission, Directorate Information Society and Media Unit A1 Audiovisual and Media Policies, Hans Bredow Institute

- Schmidt, S. & Werle, R. (1998). *Coordinating Technology: Studies in the International Standardization of Telecommunications*. Cambridge, MA: MIT Press.
- Schulz, W. and Held, P. (2001) *Regulated Self-Regulation as a Form of Modern Government*. Hamburg: Hans Bredow Institut.
- Senden, L. (2005) Soft law, Self-Regulation and Co-regulation in European law: Where do they Meet? *Electronic Journal of Comparative Law* 9:1, at <http://www.ejcl.org/91/art91-3.PDF> .
- Soete, L. (1997) *Building the European Information Society for us all. Final policy report of the High Level Group*. Brussels, DGV – Social Policy Directorate General.
- Strange, S. (1998) What Theory? *The Theory in Mad Money*, November 1998. Available from <http://www2.warwick.ac.uk/fac/soc/csgr/research/workingpapers/1998/wp1898.pdf> visited 10 June 2007
- TERENA (2006) TF-CSIRT. Available from <http://www.terena.org/activities/tf-csirt/>
- Thierer, A. (ed.) (2003) *Who Rules The Net?* Washington DC: Cato Institute.
- Trachtman, Joel P. (1998) *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, *Indiana Journal of Global Studies* Volume 5 Issue 2 Spring 1998 at 561, Indiana University School of Law – Bloomington <http://www.law.indiana.edu/glsj/vol5/no2/10tract.html> visited 22 July 1999, at 1.
- United Nations (2005) *Report of the Working Group on Internet Governance*, transmitted 14 July 2005 to the President of the Preparatory Committee of the World Summit on the Information Society, at <http://www.wgig.org/WGIG-Report.html>
- Zittrain, J. (2003). *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, Chapter 2, pp13-30 in Thierer, A. (Ed.) *Who Rules The Net?* Washington D.C: Cato Institute.